DATA PROTECTION IN THE SCHENGEN INFORMATION SYSTEM II (SIS II)

A High Level of Security within the EU Area of Freedom, Security and Justice

University of Oslo

Faculty of Law

Candidate number: 8011

Supervisor: Dr. Stephen Karanja

Co-supervisor: Dr. Yue Liu

Deadline for submission: December 6, 2010

Number of words: 17 923 (max. 18.000)

30.11.2010

Content

1 Introduction.

1.1 Background, Schengen Agreement, Schengen Convention and SIS. Emergence of the problem.

The fundamental right to free movement is among the main reasons for abolishing checks and controls at the countries' borders included in free movement areas.[1] The European Union's Internal Market[2] is dedicated to guaranteeing the free movement of persons, goods, services and capital and to build up common policies which make their movement easy and with as few obstructions as possible. The free movement attracts the need for additional or compensatory measures in order to ensure security by preventing and combating illegal activities.

Meanwhile the technological developments[3] lead to the emergence of more sophisticated tools for data collection, data storage and data processing for control and surveillance purposes. Their use exposes the easy and often unnoticeable intrusion on the data subjects' fundamental rights to privacy and data protection. Concomitantly in a democratic society adequate measures and standards

---

[1] For example, after the creation of Irish Free State in 1922, an informal agreement between the governments of Britain and Ireland established an open border area; or the creation of the Nordic Passport Union in 1952 to permit free travel amongst the Nordic countries.

[2] The EU Internal Market was established by the Single European Act signed in 1986.

[3] Bygrave, Lee A. *Data Protection Law: Approaching its rationale, Logic and Limits*, Kluwer Law International (2002), p.165 among the factors influencing the existence of data protection laws is the technological and organizational developments in the processing of personal data.

guaranteeing data protection are needed to ensure the optimal balance between personal data protection and security.

The Schengen area[4] was established with the adoption of the Schengen Agreement in 1985[5] and the Schengen Convention (CIS) adopted in 1990.[6] The signatory countries agreed to enhance the external border controls in order to combat crime and illegal immigration. The Schengen Information System (SIS)[7] was introduced by the CIS and has been operational since 1995. The SIS is a compensatory measure for the area without internal border checks and controls. It is an EU large scale IT system, which allows competent authorities in Member States[8] to exchange information used for performing controls on persons and objects at the external borders, or on their territories, as well as for issuance of visas and residence permits.[9]

---

[4] All European Union members, except Bulgaria and Romania, are members of the Schengen area. Norway, Iceland and Switzerland, non EU members, are also in the Schengen area. Two EU members, the United Kingdom and Ireland, have opted not to fully participate in SIS.

[5] The Schengen Agreement was negotiated and signed by five of the ten member states of the European Community in 1985: Belgium, France, Luxembourg, the Netherlands and West Germany.

[6] Convention Applying the Schengen Agreement of 14 June, 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany, the French Republic on the Gradual Abolition of Checks at Their Common Borders, 1990.

[7] Title IV, Articles 92-119, CIS.

[8]The term 'Member States' should be taken to include the countries which are in the Schengen area and apply the *Schengen acquis.*

[9] Opinion of the European Data Protection Supervisor on the proposals for a Council Decision[…] (COM(2005)230 final) and for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and for […] a Regulation […] regarding access to SIS II by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final), OJ C 91/38, 19.4.2006, p.1.

CIS was included in the EU legal framework [10] by the Treaty of Amsterdam, signed in 1997. The Schengen Agreement has lost the status of an intergovernmental treaty and was included into the EU legislative rules.[11] It became part of the *acquis communautaire*.[12]

Part of the Schengen provisions (immigration and refugees) fell into the first pillar (community pillar), and the other part remained in the third pillar (police and judicial cooperation). This two - pillar embracement has in fact led to two sets of rules on data protection under the first pillar and under the third pillar respectively. The system has been operational for 15 years and it has attracted a lot of criticism from academia, EU institutions and international organizations for its lack of democratic control and respect for fundamental human rights.[13] The problem that emerged with the current SIS has been related to the prevalence of security concerns over the right to privacy and the right to data protection (both terms are used interchangeably in this study).

The human rights prospective for high data protection standards established in the EU countries by the adoption of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard

---

[10] Protocol integrating the Schengen acquis into the framework of the EU annexed to the Treaty of Amsterdam, 2 October, 1997.

[11] *Ibid.*, Article 1: "This co-operation [under the Schengen agreements] shall be conducted within the institutional and legal framework of the European Union and with respect for the relevant provisions of the TEU and of the TEC."

[12] *Acquis communitaire* is the accumulated legislation, legal acts and court decisions which constitute the EU law. *The Shengen acquis* is part of it.

[13] Karanja, Stephen K. (2000), *The Schengen Cooperation: Consequences for the Rights of EU Citizens*, "Mennesker og rettigheter Årgang 18 Nr. 3 2000" , p. 215 - 222. It reflects many aspects of the current situation with SIS and SIS II; Michael, Katina and M.G, Michael, *Schengen Information System II: the balance between civil liberties, security and justice*, available at: http://works.bepress.com/kmichael/53/ , accessed on 17.7.2010 .

to the processing of personal data and on the free movement of such data (Directive 95/46/EC)[14] has been undermined. Bygrave, L. described the Directive as "the most comprehensive and complex of the instruments"[15] in the area of data protection not only inside but also outside of the EU. The exchange of personal data for police cooperation enjoyed loose standards for data protection. In this sector Member States have relied on the non-binding Recommendation No. R (87) 15 of the Committee of the Ministers of the Council of Europe of 17 September 1987. Karanja stated that the merit of CIS is in the introduction at national level of minimum data protection standards of the CoE Convention in all Member States. Concomitantly "data protection provisions in CIS have serious bottlenecks that will continue to undermine individual protection." He mentioned some serious flaws - the finalities for registration into the system are vague and wide, the personal data might be registered for many different reasons from those stipulated by CIS, also the personal data might be used for different purposes.[16]

The Treaty of Amsterdam announced the establishment of Area of freedom, security and justice (AFSJ) with a view to ensure the free movement of persons and offer a high level of protection to citizens. It covers policy areas ranging from the management of the EU's external borders to judicial cooperation in civil matters and police and judicial cooperation in criminal matters and including asylum, immigration and the fight against crime. Thus, it comprised the first pillar and the third pillar of the European Union. The AFSJ has been influenced by the political developments outside and inside Europe. And with the programmes for EU Justice and Home Affairs and internal security, namely: the Tampere programme (1999-

[14] OJ L 281/31, 23.11.1995.

[15] Bygrave, L., *Supranote* 3, p.30.

[16] Karanja, S., *Supranote 13*, p.7-8.

2004), the Hague program (2004-2009) and the Stockholm program (2010-2014),[17] it has been constantly developed reflecting the growing security concerns of the European politicians and lawmakers.

Schengen Information System second generation (SIS II) will be introduced soon. It will replace SIS. The aim of this study is to analyse the legal rules of SIS II, the exchange of information and the data protection safeguards. On this basis a conclusion will be made on whether security concerns still prevail over the personal data protection standards in the new system.

1.2 Legal method, legal approaches and difficulties.

The analyses will be done through a description of the rules of SIS II as they were adopted and an assessment of them in light of the standards for data protection that have already been established in Europe.

The main questions framing the discussion as points of departure are:

- The legal basis of SIS II, its relation to the other data protection rules, the political developments that influenced the introduction of new functions of the system;
- The anticipated impact on the right to privacy and, more specifically, on the right to data protection estimated on the basis of the data protection rules of the new legal instruments, their expected effectiveness and the anticipated tendencies in the personal data protection standards;
- Do the legal tools of SIS II represent a consistent level of data protection with that of Directive 95/46/EC in the first pillar? How do SIS II legal

[17] The Tampere Summit Conclusions, 15-16 October 1999 (the Tampere Programme); The Presidency Conclusions, 4-5 November 2004 (the Hague Programme); The Stockholm Programme - An open and secure Europe serving and protecting the citizens, 2 December 2009.

instruments include the CoE Convention rules in the third pillar? Keeping in mind that both Directive 95/46/EC (Article 3 (2) supported by Article 13) and the CoE Convention (Article 9 (2) a)) exclude the processing of personal data if carried out as part of activities in the scope of police and judicial cooperation. Analyses of the standards for data protection in SIS II under the first and the third pillar of the EU will be done by tracing the data protection rules of the new legal instruments and the new system's functions.

- The SIS II purpose to ensure a high level of security within the AFSJ - as stated in Articles 1(2) of Regulation 1987/2006/EC[18] and Decision 2007/533/JHA[19] on establishment, operation and use of the new SIS II – will be discussed briefly in order to sketch the development of the security notion in Europe.

The legal method followed here is the description of the legal rules of SIS II, supported where possible by the experience with the current SIS, and an analysis of other available text materials considered of relevance in the discussion on security and data protection.

As far as the legal analysis of *de lege lata* and *de lege ferenda* is concerned, which is respectively the law and its validity assessed in accordance with the rules as they are adopted and in accordance with what they would have to be to better serve the social needs in question, it will be attempted to make a conclusion in relation to SIS II. Nonetheless, this will be a difficult venture since there is no case law and no practice with SIS II. However, case law at the national level of the Member States and current SIS practice would be used.

[18] OJ L 381/4, 28.12.2006.

[19] OJ L 205/63, 7.8.2007.

The following are the theoretical approaches of this discussion, representing the summary of the answers to the framework questions as posed above.

- Accepting and justifying the *status quo* prioritizing security concerns and measures over the protection of personal data in SIS and keeping it in SIS II by virtue of the justification of "the war against terrorism and fight against organized crime"; and
- Looking at high level of security and data protection as two variable sides of one coin that inevitably exist together, at least as long the political and social developments dictate so. The prevalence of one of them or striking adequate balance between them is justified on a case by case basis thus ensuring their optimal proportion in a specific situation in a democratic society.

Both theoretical approaches will help to portray the interrelationship between security and data protection in SIS II and to illustrate whether it is possible "to maximize the two values instead of pitting them against each other." [20] The aim will be to present the interrelationship between security and data protection and the main factors that influence it.

The difficulties in this study are related firstly to the concepts of right to privacy and right to data protection on the one hand and security on the other. The right to data protection is primarily related to an individual[21] while security primarily concerns a community consisting of individuals. The concepts of privacy and security are interpreted and understood differently in different situations and cultural traditions thus their content and limits could not be universally defined. A

[20] Karanja, S., *The Directive on Data Retention-Between Privacy and Security*,YULEX 2006, pp.49-62, p.63.

[21] Bygrave, L. *Supranote* 3, Chapter 7, p.125.

country's specific political, economic and social developments influence them.[22] In SIS II, both concepts relate to different countries which have different levels of political, economic and social development.

There is no practice with SIS II. The research will be done on the basis of its legal rules and sometimes on guess work. A useful source of information will be the practice with SIS since SIS II is going to continue its tasks.

The lack of judicial decisions concerning the operation of SIS II is an additional hurdle for this research. The SIS judicial decisions at national level could be of help.

Literature that will be used includes: the binding and non binding documents adopted within the EU that are relevant to this study, the opinions of, for example, the European Data Protection Supervisor (EDPS), the Joint Supervisory Authority Schengen (JSA), as well as articles written by Stephen K. Karanja, and his book "*Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*" (2008); also the books of Els De Busser "*Data Protection in EU and US Criminal Cooperation*", (2009); Evelien Brouwer "*Digital Borders and Real Rights Effective Remedies for Third-Country Nationals in the Schengen Information System*", (2008); Lee A. Bygrave "*Data protection Law: Approaching Its Rationale, Logic and Limits*", (2002) and where considered appropriate, other text materials. All these will be analyzed by relating their respective parts to the main points of this study: SIS II and the interrelationship between security and data protection.

[22] Karanja, S. *Supranote 20*, p.49.

1.3 Chapters overview.

Next chapter will present what conditioned the establishment of the SIS II data base: the political developments such as terrorist attacks and threats which influenced the security measures in the current SIS and in the future SIS II. The personal data protection rules in SIS II, as well a brief look at its structure, architecture and purpose. Chapter 3 discusses in a nutshell the concept of personal data according to the SIS II legal instruments, the new data protection rules, and focuses on some problems of data protection in SIS II with a summing up. The new functions and the problems they pose to data protection in SIS II with a short summing up are discussed in the fourth chapter. Chapter 5 will propose a summarized conclusion on the interrelationship between security and data protection based on recently adopted legal and non legal documents in the EU having reference to SIS II.

2 SIS II database.

2.1 The need for SIS II. Legal texts.

The need for SIS II became apparent in the beginning of the functioning of SIS. During a meeting in December 1996 the Member States decided to develop SIS II[23] in the context of the EU enlargement and the limited technical capacity of SIS. Concomitantly, in the following years there were other political developments that in turn accelerated the idea of including the most advanced technological solutions for surveillance and control into the future system. [24]

Many authors and organizations see the emergence of new threats to the right to privacy. [25]

The development of SIS II has been entrusted to the Commission pursuant to Council Regulation 2424/2001 of 6 December 2001[26] and Council Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II).[27] Both legal instruments constitute the necessary legislative basis for governing SIS II in respect to matters falling within the scope of the Treaty on

---

[23] Schengen acquis, SCH/Com-ex (97) 2 rev.2, p. 540 and SCH/Com-ex (97) 24, p.543.
OJ L 239, 22.9.2000.

[24] Communication from the Commission […], Development of the Schengen Information System II, COM (2001) 720, final, Brussels, 18.12.2001, p.3.

[25] Hayes, B. (2005) Statewatch Analysis, SIS II: fait accompli? Construction of EU's Big Brother Database Underway, also Michael, Katina and M.G, Michael, Schengen Information System II: the balance between civil liberties, security and justice, available at: http://works.bepress.com/kmichael/53/ , accessed on 17.7.2010. and organizations like Privacy International: http://www.privacyinternational.com; Statewatch: http://www.statewatch.org; European Digital Rights: http://www.edri.org

[26] OJ L 328, 13.12.2001, p.4-6.

[27] OJ L 328, 13.12.2001, p.1-3.

EU (TEU) and the Treaty of EC (TEC). Later on a package of two Regulations and one Decision was adopted:

- Regulation 1987/2006/EC (SIS II Regulation);
- Council Decision 2007/533/JHA (SIS II Decision) and
- Regulation 1986/2006 of the European Parliament and of the Council

regarding access to the Second Generation Information System by the services in the Member States responsible for issuing vehicle registration certificates, based on Title V (Transport) of the TEC (Regulation 1986/2006). [28] The latter will not be discussed in length in this study.

The principle is that SIS II constitutes one single information system despite the fact that it is governed by separate instruments because of its two-pillar embracement – the first pillar and the third pillar.

The first pillar includes the immigration aspects of SIS II - visas, asylum immigration and other policies related to the free movement of persons of the TEC. The third pillar includes the use of SIS II for purposes of police and judicial cooperation in criminal matters of the TEU, (Recitals 3 and 4 of the SIS II Regulation and Decision).

Other legal instruments discussed in this study are:

Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Framework Decision 2008/977/JHA),[29] a third pillar legal

[28] OJ L 381/1, 28.12.2006.

[29] OJ L 350/60, 30.12.2008.

instrument; Regulation 45//2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (Regulation 45/2001)[30] which encompasses all data processing activities of the Commission in SIS II; Directive 95/46/EC which is strictly a first pillar legal instrument and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28.01.1981 (CoE Convention). All Member States have ratified it and adopted data protection laws at national level and the non-binding Recommendation R (87) 15 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector.

All of the above mentioned legal instruments acquired positions of general and specialized legal rules in relation to each other or *"lex specialis"* to *"lex generalis"*.[31]

The legal rules on establishment, operation and use of SIS II and their relation to each other are complicated by the two-pillar structure kept in the system despite the fact that many Schengen commentators have advocated for the transfer of *the Schengen acquis* to the first pillar.[32]

The complexity of the legal rules also is conditioned by historical reasons and by overall political developments. The first adopted among the all data protection instruments having binding nature for the signatory countries is the CoE Convention. It set the general data protection principles which became the

---

[30] OJ L 8/1, 12.1.2001.

[31] EDPS, *Supranote 9,* p. 41.

[32] Karanja, S. (2008), *Transparency and Proportionality in the Schenegen Information System and Border Control Co-operation,* Martinus Nijhoff Publishers, 2008, p.421.

minimum threshold for data protection. They have been further developed by the adoption of Directive 95/46/EC and later by Regulation 45/2001/EC, where more up to date rules were implemented.

2.2 Political Developments.

There were political developments with major significance for the western democracies. They influenced not only the overall notion for security with the leading role of the USA after September 11, 2001 (9/11),[33] but in particular the shape and the functions of SIS II. In its Working Paper on the Development of SIS II the Commission concluded that a clear political and financial support for the building up of a new, flexible system based on modern technology is needed not only because new users will be included but also in light of events such as those of 9/11. [34]

The terrorist threats and attacks are a relatively new piece on the political landscape in many western countries.[35] The attacks which happened in the USA and Europe[36] have triggered the process of widening police and surveillance powers at the expense of protection of right to privacy and data protection.[37] They have been used

[33] Mironenko, Olga (2009), Air *Passenger Data Protection, Data Transfer from the European Union to the United States*, submitted as a Master Thesis in the University of Oslo in autumn 2009.

[34] Commission Staff Working Paper on the Development of the SIS II, 2002 Progress Report, Brussels 18.2.2003, SEC (2003) 206, p.13.

[35] The European Community members in 1975 established an intergovernmental cooperation framework - TREVI (Terrorism, Radicalism, Extremism, and Violence). It allowed information exchange and occasional cross-border coordination of measures to prevent and combat terrorism.

[36] September 11, 2001 in the USA, Madrid in 2004 and London in 2005.

[37] Karanja, S., *Supranote 32*, p. 64.

as justification for strengthening the security measures and shaped the aims of the European AFSJ.

Statewatch, an independent non-profit making organization which monitors the state and civil liberties in Europe observed that there has been at the EU level (as well as the national level) an avalanche of new measures, practices, databases, etc., most of which have very little to do with countering terrorism and rather concern-crime in general, the targeting of refugees, asylum seekers, the resident migrant population, etc.[38]The organization made similar observation in relation to counter terrorist measures and their relevance with tackling terrorism, after the attacks in Madrid in 2004. It identified at least 57 such measures and stated that 27 of the proposals have nothing or little to do with tackling the terrorism but would introduce the wholesale surveillance on everyone in Europe and could potentially be used for social and political control. [39]

SIS has not been left behind in this tendency and the right to data protection has been lagging behind the security concerns.[40] The Conclusions of the Laeken European Council of 14 and 15 December 2001 and in particular Conclusions 17 (cooperation between specialised counter-terrorism services), 43 (Eurojust and police cooperation with regard to Europol) and the Action Plan of 21 September 2001 against terrorism refer to the need to enhance SIS and improve its capabilities. Under the initiative of Spain Council Decision 2005/211/JHA of 24 February 2005[41] and Council Regulation 871/2004 of 29 April 2004 were adopted concerning the introduction of some new functions for SIS, including the fight

---

[38] Bunyan, T., Statewatch (2002), *The War on Freedom and Democracy: An analysis of the effects on civil liberties and democratic culture in the EU,* 6.9.2002, available at: http://www.statewatch.org/news/2002/sep/analysis13.htm, accessed on 28.06.2010.

[39] Hayes, B., Peers, S. and Bunyan,T., Statewatch (2004), *Scoreboard on post -Madrid counter-terrorism plans,* 23 March 2004, p.1, points 2 and 3.

[40] Karanja, S., *Supranote 32*, p. 64.

[41] OJ L 68/44, 15.3.2005.

against terrorism.[42] Both of these introduced amendments to the CIS with a view to enhance the role of SIS in this field.

The data protection standards according to the SIS II legal instruments are split into the two pillars of the EU as with SIS according to CIS.[43] There will be two levels of protection of personal data in SIS II, one lower under the third pillar and one relatively higher under the first pillar for gathering and processing of personal data.[44] The *status quo* is not only maintained, but further developed by the introduction of new functions and the use of the most advanced technologies in SIS II justified by the EU enlargement and the need for effective security guarantees.

2.3 Structure, architecture and purpose of SIS II.

For a better understanding of the interrelationship between security and data protection in SIS II it would be useful to take a brief look at its structure, architecture and purpose.

2.3.1 Structure of SIS II.

SIS II has a central system Central SIS II, which is composed of a technical support function ('CS-SIS') containing the SIS II database to which all Member States will have access and a uniform national interface ('NI-SIS"). In each of the Member States a national system (N.SIS II) is established. N.SIS II is consisting of the national data systems to which the competent national authorities of the concerned

---

[42] OJ L162/29, 30.4.2004.

[43] CIS requires a minimum data protection level equivalent to that in the CoE Convention and in the exchange of data in the police cooperation Member States have to comply with the Recommendation R (87)15 (Article117).

[44] Karanja, S., *Supranote 32*, p. 424.

Member States will have access. They communicate with Central SIS II. Between CS-SIS and NI-SIS there is 'Communication Infrastructure' that provides an encrypted virtual network dedicated to SIS II data and to the exchange of data between SIRENE Bureaux (an acronym for Supplementary Information Request at the National Entry). The SIRENE Bureaux are not part of SIS II. They are designated by each Member State. They ensure the exchange of all supplementary information and shall also coordinate the verification of the quality of the information entered in SIS II.[45] So as a whole the structure of SIS II is composed of three main parts - CS-SIS; N.SIS II and Communication Infrastructure, and one additional – SIRENE Bureaux, through which information will flow.

The establishment of SIRENE Bureaux was determined on the grounds that very often the details entered into SIS under CIS Article 94 (3)[46] are not enough to give the authorities the information they need. The supplementary information of all national databases which is not entered in C.SIS is accessible upon request to law enforcement agencies in all Member States. SIRENE Bureaux have no legal basis in CIS but without it SIS could scarcely function.[47] They function in accordance with the SIRENE Manual.[48]

2.3.2 Architecture of SIS II.

The way that SIS II will function is to allow the Member States to contribute data on people wanted for arrest, surrender or extradition, people wanted for judicial procedures, people to be placed under surveillance or subject to specific checks,

---

[45] Articles 4 of the SIS II Regulation and Decision.

[46] CIS, Article 94(3) requests that only "alphanumeric" data (letters and numbers) are to be stored in SIS.

[47] House of Lords EU Committee 9th Report on Session 2006-07, paras 53-55, p. 19.

[48] Decision 2006/758/EC on amending the Sirene Manual, OJ L 317/41,16.11.2006.

people to be refused entry into the Schengen area and data on stolen or lost items. The data processed through the current C.SIS are quite numerous as shown in the Annex 2 (statistics for 2007, 2008 and 2009).[49] Logically, after the integration of 9 new Member States in September 2007 these numbers show an upward tendency. Consequently it will lead to an increased number of hits as it was pointed out by the SIS/SIRENE Working Party/Mixed Committee (see also Annex 3).[50] The new functions of SIS II, based on the latest technological solutions, change its capacity and effectiveness and the number of hits will grow which will negatively affect the possibility for personal data protection (see Chapter 4).

2.3.3 Purpose of SIS II.

The purpose of SIS II is stated in Articles 1 (2) of the SIS II Regulation and Decision and it is "to ensure a high level of security within the area of freedom, security and justice of the European Union […], and to apply the provisions of Title IV of Part Three of the EC Treaty relating to the movement of persons in their territories, using information communicated via this system." In general, it keeps the same purpose as the current SIS to ensure security and to apply the relevant provisions of the Treaty on the free movement of persons using information transmitted via the system (CIS, Article 93).[51] However, in the part related to security: "a high level of security within the area of freedom security and justice of the EU" is proscribed, while in Article 93 of CIS it is "[…] to maintain public order

[49] MEMO/10/349, Brussels, 20 July 2010, EU Information Management Instruments, p.3.

[50] Council of the EU, 5171/09, LIMITE, SIRIS 7, COMIX 22, Brussels, 19 February, 2009.

[51] Article 93 of CIS: "The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public order and security, including State security, and to apply the provisions of this Convention relating to the movement of persons, in the territories of the Contracting Parties, using information transmitted by, the system."

and security,[…].” Thus, there is tendency of giving higher prominence to security matters in SIS II.[52]

The high level of security is one of the main goals of the EU. The Amsterdam Treaty explicitly mandates the EU to provide EU citizens with it (Articles 29 TEU and 61 (e) TEC). The Member States’ competences in internal security remain predominant. The competences of the EU are in the external security (i.e. in the relations of the EU with other organizations or third states). According to the principle of subsidiarity the EU can acquire some competences on internal security issues (if at EU level the cross-border threats to security can potentially be more effectively handled through common action). All issues concerning security, in the third pillar, are primarily resolved through cooperation between the Member States. This cooperation is established among different national systems that are largely autonomous and substantially different. Thus, in the third pillar the legislative harmonization of data protection in SIS is kept at a low level, with the requirement that the Member States observe the main principles of data protection. The assurance of a high level of security concerns not only the third pillar but also the first pillar in the course of gathering and processing of data in SIS II (see Chapter 4).

[52] Karanja, S. (2005), *SIS II Legislative Proposals 2005: Gains and Losses!*, YULEX 2005, p.82.

3 The problems of data protection in SIS II.

3.1 Concept of Personal data in SIS II.

The SIS II Regulation and Decision provide a definition for personal data in their Articles 3, e): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly." Thus personal data is defined in a broad and flexible way following the definitions given by the first legal instruments in Europe the CoE Convention, Directive 95/46/EC and also the Organization for Economic Co-operation and Development (OECD) Guidelines.[53] In 2007 the Article 29 Working Party of Directive 95/46/EC (Article 29 WP) published an opinion on the concept of personal data[54] of Directive 95/46/EC. The Article 29 WP is composed of a representative of national supervisory authorities of the Member States, has advisory status and acts independently. The objective of the analysis is "to come to common understanding of it [concept of personal data] since this is tantamount to defining what falls inside or outside the scope of data protection rules."[55] It is closely related to the definitions of personal data in the CoE Convention and OECD Guidelines both of which define it in similar terms as Directive 95/46/EC (Article 2, a)) - "any information relating to an identified or identifiable individual (data subject)." The Article 29 WP noted that the term "any information" in the Directive clearly signals the willingness of the legislator to design a broad concept of personal data."[56]

---

[53] Cf. Article 2, a) of the CoE Convention; Article 2., a) of Directive 95/46/EC and Part one, General definitions, second intend of OECD Recommendation of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data

[54] Article 29 Data Protection Working Party, 01248/07/EN, WP 136, Opinion 4/2007, 20.6.2007, p.p.6-9.

[55] *Ibid.*, p.3.

[56] *Ibid.*,p. 6.

The broad notion of personal data is adopted in the SIS II legal instruments and harmonized with the definition of personal data given by the CoE Convention and Directive 95/46/EC.

This differs from the definition of personal data in CIS, Article 94 (3) where it is given by exhaustive lists of information for persons and Article 100 (3) on objects. Following the logic of the Article 29 WP, the scope of data protection rules is delineated by the lists of data that shall be entered in SIS. Other data are excluded since they are not considered personal under CIS.

The adoption of the broad and flexible notion about personal data in the SIS II rules is a positive sign from the point of view of its harmonization and unification among the Member States and from the point of view of the scope of application of data protection rules. The categories of data according to the SIS II legal instruments are on persons and objects (Articles 20 (2) of the SIS II Regulation and Decision). Both categories are personal data - the data on persons provides information for direct indirect and those on objects for indirect identification of a natural person.[57]
In this study the main focus is on information on persons in SIS II.
The flexible and broad notion of personal data is restricted by the wording "The information on person […] shall be no more than the following" (Articles 20 (2) of the SIS II Regulation and 20 (3) of the SIS II Decision), which limits the personal data to the stated lists of information.[58]

---

[57] Karanja, S. concluded that both categories of data are personal data, *Supranote 32*, p.142.

[58] Articles 20 (2) of the SIS II Regulation and (3) of the SIS II Decision:
"a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; b) any specific, objective, physical characteristics not subject to change; c) place and date of birth; d) sex; e) photographs; f) fingerprints; g) nationality(ies); h) whether the person concerned is armed, violent or has escaped; i) reason for the alert; j) authority issuing the alert; k) a reference to the decision giving rise to the alert; l) action to be taken; m) links to other alerts issued in SIS II […]; in the SIS II Decision one more is 'n) the type of offence.'"

There is supplementary information which might be exchanged in connection to SIS II alerts through the SIRENE Bureaux. There also are additional data on persons connected with the alerts which are to be immediately available to the competent authorities. In difference with the supplementary information additional information is stored in CS-SIS II (Articles 3 b) and c) of the SIS II Regulation and Decision). Thus, it will be accessible to all Member States. Additional data which is a copy of the European Arrest Warrant (EAW)[59] will be exchanged (Article 27 of the SIS II Decision).

A disturbing aspect from point of view of personal data protection is the inclusion of biometrics (photographs and fingerprints) as it is possible to use them for purposes other than those they were initially collected for, i.e. function creep and they are not 100 % reliable for identification purposes (see Subchapter 4.2).[60] Dr von Pommer Esche from the Police Intelligence Service of the German Federal Data Protection Office expressed concern about the reliability of biometrics when used for investigative purposes and he recommended additional safeguards to be reconsidered if those data are used.[61]

---

[59] Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18/07/2002, p. 1– 20: "Article 8 (1) The EAW shall contain the following information[…]: (a) the identity and nationality of the requested person; (b) the name, address, telephone and fax numbers and e-mail address of the issuing judicial authority; (c) evidence of an enforceable judgment, an arrest warrant or any other enforceable judicial decision having the same effect, […]; (d) the nature and legal classification of the offence, […]; (e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the requested person; (f) the penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing Member State; (g) if possible, other consequences of the offence."

[60] EDPS, *Supranote 9*, para 4.1, p. 43-44.

[61] House of Lords, *Supranote 47*, p.20, para 58.

Personal data that will be entered in SIS II are of a greater quantity and quality than in the current SIS and also in comparison with the personal data according to the CoE Convention and Directive 95/46/EC. The CIS, CoE Convention and Directive 95/46/EC do not require biometrics and EAW to be entered.

3.2 Data protection in SIS II.

The right to data protection is one of the fundamental human rights. It was developed through the jurisprudence of the European Court of Human Rigths (ECtHR) related to the right to privacy in Article 8 of the European Convention of Human Rights.[62]

The Charter of Fundamental Rights of the European Union[63] for the first time directly refers to the fundamental right of everyone to protection of personal data concerning him or her (Article 8):

> Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

According to Article 52 of the Charter these rights may be subject to limitations, provided that similar conditions are fulfilled as applicable under the ECHR.

---

[62] European Convention of Human Rights, 1950.

[63] OJ C 364/3,18.12.2000.

The Charter's legal status is recognized by the EU in the Lisbon Treaty, Article 6 "1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, […], which shall have the same legal value as the Treaties.", OJ C 306/1, 17.12.2007.

The SIS II Regulation (Recital 26) and the SIS II Decision (Recital 34) state that they respect the fundamental rights and observe the principles recognized in the Charter of Fundamental Human Rights.
Data protection principles and rules for both SIS and SIS II are provided in the CoE Convention to which all Member States are signatories and in the non-binding Recommendation No.R (87) 15, both of which are applicable to the current SIS (Article 117 CIS).

The new SIS II legal instruments additionally refer to data protection rules of Directive 95/46/EC for the first pillar data processing, Regulation No 45/2001/EC for the processing of personal data by the Community institutions and bodies, and to the recently adopted Framework Decision 2008/977/JHA for the third pillar.[64] The European lawmakers aim to align the principles of data protection of SIS II with those of the other legal binding instruments of the EU. However, the new legal instruments reflect the logic of the political developments from the last decade and do not entirely implement the data protection standards and principles of the two leading instruments the CoE Convention and Directive 95/46/EC. The level of personal data protection among the Member States is considered adequate in the first pillar through the adoption of national laws in accordance with Directive 95/46/EC. However, in the third pillar the level of personal data protection is not fully in line with the CoE Convention as it is discussed later in subsections 3.2.1 and 3.2.2 and in Chapter 4. Two categories of standards – one related to the first and other related to the third pillar SIS II data processing will continue to coexist. The difference in the purposes of the two types of personal data collecting and processing preconditions their existence in SIS II.

[64] Recitals 15 and 16 of the SIS II Regulation and 19, 20, 21, and 22 of the SIS II Decision.

In the first community pillar the Member States have to adopt national legal rules achieving the results prescribed at the EU level. The ECJ has competence for interpretation of the first pillar legal instrument and the European Parliament will be involved in the process.[65]

The third pillar is intergovernmental due to the strong link to the sovereignty of the states. Thus, it is not extraordinary that many rules are left to be defined under the national law of the Member States, which leads to coexistence of variety of legal rules for one and the same personal data protection in the police and judicial affairs.

The SIS II Regulation, first pillar, and the SIS II Decision, third pillar, are *lex specialis* for data protection in SIS II. All other rules are *lex generalis*.
The interrelationship between *lex generalis* and *lex specialis* is defined by the rule *lex specialis derogat legi generali*. *Lex specialis* must be in conformity with *lex generalis* and not to be considered as exception from it. [66]

As for the supervision of personal data processing in SIS a joint supervisory authority (JSA) is set up, consisting of two representatives from each national supervisory authority (Art. 115 CIS).

The SIS II first and third pillar personal data processing activities shall be supervised by the EDPS, with the following exceptions: when the personal data are accessed and further processed by Europol and Eurojust then the supervisory authorities established by the Europol Convention[67] and the Decision establishing

---

[65] EDPS, *Supranote 9*, para 1.2., p.39.

[66] *Ibid.*, para 2.2.1, p.41.

[67] Europol Convention on the establishment of a European Police Office, replaced by Council Decision 2009/371/JHA, OJ L 121/37, 15.5.2009. The SIS II Decision refers to the Convention.

Eurojust[68] have the monitoring powers (Article 41 (5) letter e) and Article 42 (3) of the SIS II Decision). The supervision competences of the EDPS are a positive improvement from data protection perspective, since he has better defined monitoring powers than the JSA.[69] The EDPS shall cooperate with the national supervisory authorities and for this purpose they shall meet at least twice a year (Article 46 of the SIS II Regulation and Article 62 of the SIS II Decision).

The following discussion will focus on data protection rules related to the quality of data, the quality of data processing and the individual rights of data subjects according to the special legal rules of SIS II and will compare them with the general rules.

3.2.1 SIS II Regulation - quality of data, data processing and data subject rights.

In the first pillar the rules on quality of data (Article 34 of the SIS II Regulation) stipulate that the Member State issuing the alert shall be responsible for the quality of personal data, i.e. to ensure that the data are accurate, up-to-date and entered into the system lawfully, the Member State issuing the alert is authorized to modify, add to, correct, update or delete data which it has entered. If a Member State other than the one that issued the alert has evidence that an item of data is factually incorrect or has been unlawfully stored it can only inform the Member State that issued the alert through the exchange of supplementary information. In the event that the Member States cannot reach agreement, the EDPS shall act as mediator jointly with the national supervisory authorities concerned. A further alert on the same person

[68] Council Decision 2002/187/JHA setting up Eurojust […], OJ L 063, 6.3.2002, p. 1-13.

[69] Karanja, S., *Supranote 32*, p.422.

may be entered after an agreement between the first Member State that issued the alert and the Member State which entered it.

Directive 95/46/EC provides the principles related to data quality in Article 6 "[…] personal data must be: a) processed fairly and lawfully;" […]"c) and d) "adequate, relevant and not excessive in relation to the purposes for which they were collected […] ." All principles relating to data quality must have been included at national laws in accordance with Directive 95/46/EC. In this respect the special rules follow the logic of the general ones.

As for the quality of personal data processing, the purpose limitation principle is stated in Article 31(1) of the SIS II Regulation. The purposes for processing data are refusing entry into or a stay in the Member States' territories. Article 31(7) states that "any use of data which does not comply with paragraphs (1) to (6) shall be considered as misuse under the national law of each Member State." There is no exception from the purpose limitation principle, which is positive for data protection, but the new functions of SIS II have the potential to undermine this situation in the first pillar (see subchapter 4.4).

Alerts in SIS II pursuant to the SIS II Regulation shall be kept only for the time required to achieve the purposes for which they were entered (Article 29 (1)). In period of three years the Member States shall review the need to keep the data (Article 29 (2)). If the Member State decides to keep the alert then in 3 years period of time another review of the need to keep it should be made. The decision is based on a comprehensive individual assessment should this prove necessary for the purposes for which the alert was issued (Article 29 (4)). Any extension of an alert shall be communicated to CS-SIS. In other cases, alerts shall automatically be erased (Article 29 (5)). The data quality and the quality of data processing in Directive 95/46/EC (Article 6 "Principles relating to data quality", Article 7

"Criteria for making data processing legitimate") are defined in more elaborate terms than in the SIS II Regulation. The level of protection of *lex specialis* is not consistent with that of *lex generalis.* The principles relating to quality of data processing are not defined as comprehensively as in the general rules.

The individual rights of data subjects: right to access, correction of inaccurate data and deletion of unlawfully stored data are regulated in Article 41 of the SIS II Regulation. The individual right to information of data subjects defined in Articles 10 and 11 of Directive 95/46/EC, are applicable to the third country nationals who are subjects of an alert (Article 42 of the SIS II Regulation) this is a positive sign for data protection. [70] The right to information is narrowed by the exceptions that do not exist under Directive 95/46/EC - information shall not be provided where the personal data have not been obtained from the third country national and the provision of the information proves impossible or would involve a disproportionate effort, where the data subject has the information and where national law allows for the right to information to be restricted (Article 42 (2)). All exceptions at national level are supposed to be in line with those of Directive 95/46/EC thus the SIS II Regulation provide additional exceptions from the right to information to those in Directive 95/46/EC (Article 13).

The data subjects may bring action before the courts or an authority competent under the law of any Member State (Article 43 of the SIS II Regulation). The individual rights of data subjects and the procedures for their exercise will be regulated at national level. Directive 95/46/EC also refers the regulation of the individual rights to the national law of Member States (Article 22). The difference is that in SIS II the data subjects in the first pillar are third country nationals often

[70] Karanja, S., *Supranote 52*, in the CIS it is difficult for data subjects to know which is the Member State that issued an alert, p.98.

residing outside the Schengen area. There will be differences among the rules in different Member States and third country nationals will be in a difficult position since they will have to be familiar with the rules and procedures of the concerned Member State.

The difference between the SIS II Regulation and Directive 95/46/EC is quantitative and qualitative. The detailed and comprehensive rules of *lex generalis* are not fully followed up on in *lex specialis.* There are additional exceptions from the individual rights of data subjects, which undermine the level of personal data protection as it is provided in Directive 95/46/EC. The position of the data subjects as third country nationals is not properly reflected as far as remedies are concerned. The rules on data protection for SIS II in the first pillar are closer to the level of protection provided by Directive 95/46/EC than in SIS but still not consistent with them.

3.2.2 SIS II Decision - quality of data, data processing and data subject rights.

In the third pillar Article 49 of the SIS II Decision provides the same rules on data quality and processing in SIS II as those of the first pillar SIS II Regulation.

According to the general rules of Framework Decision 2008/977/JHA (Article 8), the transmitting Member State verifies the quality of personal data and in the event that incorrect data have been transmitted or data have been unlawfully transmitted, the recipient must be notified without delay and the data must be rectified, erased or blocked without delay in accordance with Article 4.

As to the quality of data processing in the third pillar, personal data may be collected only by the competent authorities and only for specified, explicit and legitimate purposes and processed only for the same purpose for which they were collected (Article 46 (1) of the SIS II Decision and Article 3 (1) of Framework Decision 2008/977/JHA). Framework Decision 2008/977/JHA in Article 3 (1) second sentence specifies that the processing of data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which the data were collected. This is in line with the general rules on quality of data enshrined in Article 5 of the CoE Convention. Thus, the principle of purpose limitation in SIS II is stated in *lex specialis* – the SIS II Decision and *lex generalis*- Framework Decision 2008/977/JHA. Both legal instruments provide exceptions from this principle. Exceptions and restrictions are allowed in accordance with Article 9 of the CoE Convention, which is part of *lex generalis* to the SIS II legal rules in the third pillar.

Article 46 (5) of the SIS II Decision provides that data might be processed for purposes other than those for which it was entered in SIS II if it is linked with a specific case and justified by the need to prevent an imminent serious threat to public policy and public security, on serious grounds of national security or for the purposes of preventing a serious criminal offence. In any case prior authorization from the Member State issuing the alert must be obtained. This can be lawful on the basis of Article 9 of the CoE Convention, since a link to a specific case is needed and the necessity requirement is included.[71] However, the new functions of SIS II have the potential to undermine the application of the purpose limitation principle (see Chapter 4).

[71] De Busser, Els, (2009), *Data Protection in EU and US Criminal Cooperation,* Maklu 2009, p.155.

More disturbing from a data protection point of view are the general rules to SIS II in the third pillar in particular Framework Decision 2008/977/JHA. The exceptions from the purpose limitation principle are formulated in Articles 3 (2) and 11. Article 11 is applicable in accordance with the requirements of Article 3 (2), i.e. the further processing is not incompatible with the purposes for which the data were collected, the competent authorities are authorized to process such data for such other purposes and the processing is necessary and proportionate to that other purpose. Among other exceptions provided in Article 11 is the exception in indent d) "any other purpose […]" on the condition that the transmitting Member State or the data subject gives their consent and in accordance with the national law. This exception opens almost unlimited possibility for further processing. The EDPS pointed out that the consent of the transmitting Member State does not provide legal grounds to derogate from the purpose limitation principle and that this broad derogation does not fulfill the basic requirements of adequate data protection and even contradicts the basic principles of the CoE Convention.[72] De Busser, E. made the conclusion that as a general legal instrument for all judicial and police cooperation in criminal matters the inclusion of this wide formulation of purpose limitation has a detrimental effect on the efforts made in order to protect personal data in the EU.[73]

The retention period of alerts under Article 44 (1) of the SIS II Decision is defined by the time required to achieve the purposes for which they were entered. The same review procedure of the need to keep the data as in Article 29 of the SIS II Regulation applies for the third pillar (Article 44 (2), (4) and (5) of the SIS II Decision).

---

[72] EDPS, 3rd opinion on the Proposal for a Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters, OJ C, 139/1, 23.6.2007, para 23, p.5.

[73] De Busser, *Supranote 71*, p.104.

According to the general rules appropriate time limits for erasure and review of personal data shall be established (Article 5 of Framework Decision 2008/977/JHA). Article 4 (2) states that personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or were lawfully further processed. Concomitantly, they can be archived in a separate data set for an appropriate period in accordance with national law. Thus, different periods will coexist among the Member States. The general rules of Framework Decision 2008/977/JHA stipulate data protection principles in general terms and provide wide exceptions as the possibility for further use of those data which is a derogation from the purpose limitation principle. Thus, Framework Decision 2008/977/JHA does not meet the data protection standards of the CoE Convention. In particular, the possibility of processing data for any purposes other than those for which they were transmitted and the retention of erased or anonymous personal data beyond the appropriate time period are contrary to the purpose limitation principle.

The individual rights of data subjects – right to information and right of access - are to be defined in accordance with the national law of the Member States (Article 58 (1) and (2) of the SIS II Decision and Article 16 (1) of Framework Decision 2008/977/JHA). Information shall not be communicated to the data subject when the Member State which issued the alert has not given its consent. It shall not be communicated if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties (Article 58 (3) and (4) of the SIS II Decision). A similar restriction of the individual right to information is provided by Framework Decision 2008/977/JHA (Article 16 (2)). The Member States may adopt legislative measures restricting access to information, where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure

for the purposes stated in Article 17 (2) a) to e) of Framework Decision 2008/977/JHA.

Both legal instruments in the third pillar leave the regulation of the exceptions from the individual rights of data subject to the national law of the Member States. The data subjects may invoke their right of access to data relating to them on the territory of a Member State according to Article 58 (1) of the SIS II Decision. The data subjects shall be advised that they may appeal to the national supervisory authority, a judicial authority or to a court when they receive refusal or are restricted from access without communication in writing according to Article 17 (3) of Framework Decision 2008/977/JHA. The same reasoning as for Article 58 (1) of the SIS II Decision applies.

Both legal instruments provide remedies for the data subjects at national level where different rules and procedures among the Member States apply. This would create difficulties for the data subjects.

3.3 Summing up.

The data subject may easily experience a violation of his/her right to data protection in SIS II. Their other fundamental human rights might be restricted unlawfully as well, for example right to free movement within the Schengen area when an alert is entered into the system.

The data protection rules in the first pillar of the SIS II special rules are not consistent with the basic legal principles established by Directive 95/46/EC. They are stated in general terms, include more exceptions than Directive 95/46/EC and are left to the Member States national law. The third countries nationals' position is not fully taken into account and they might experience difficulties when they need

remedies for breach of their right to data protection. The positive element for data protection is that there are no exceptions from the purpose limitation principle. Another positive step is the right to information. But both may be undermined by the new functions of the system and the exceptions provided at national level.

The legal instruments of the third pillar processing of personal data in SIS II do not provide data protection principles in their full scope. The violation of the purpose limitation principle is detected through the Member States' competent authorities' possibilities to use personal data for purposes different from those they were initially entered for and to retain personal data without time limits. As a whole, data protection has not been developed in this field and the CoE Convention's data protection principles are not followed. They need to be adopted in the national laws of the Member States and different interpretations and definitions will coexist.

The *status quo* of prevalence of security concerns is prolonged and even further elaborated in the SIS II data processing provisions - the data protection standards to which the European countries claim to adhere have not been reproduced entirely in the SIS II *lex specialis*.
In the third pillar *lex generalis* Framework Decision 2008/977/JHA provides for wide exceptions to the principle of purpose limitation and an option for retention of erased or anonymous data beyond the appropriate period of time.

What is positive from a personal data protection perspective, in both of the SIS II special legal instruments, is the adoption of a harmonized concept of personal data in accordance with the other European legal instruments. Also, there is an option for the Member States to establish shorter review periods in their national laws, and to keep personal data for as short a time as possible. They have an obligation to keep statistics about the number of alerts whose retention period has been extended (Articles 29 (3) and (6) of the SIS II Regulation and 44 (3) and (6) of the SIS II

Decision). This benefits the supervision and control work. Another positive is the competence of the EDPS together with the national supervisory authorities to supervise SIS II, since the EDPS has well defined monitoring powers.

SIS accommodates great numbers of personal data and hits (see Annexes 2 and 3). The forthcoming system will accommodate even greater numbers of personal data, since the personal data to be registered in SIS II are of greater quantity and quality than those in SIS. Logically, it was expected that with the new legal instruments adequate safeguards for personal data protection will be introduced. The result does not seem satisfactory.

The new functions of the system will expand enormously its efficiency and capabilities in personal data gathering and processing. This is not a positive development for personal data protection since there are not adequate safeguards, as shown in the following chapter.

4 New functions of SIS II and data protection.

The new functions, based on the most advanced technological solutions, change the main characteristics of the system and have the potential to undermine the main principles of data protection adopted in the CoE Convention and Directive 95/46/EC.

The new functions accommodated by SIS II are formulated in short by Ben Hayes,[74] as follows:

> (i) the addition of new categories of alert;
> (ii) the addition of new categories of data, including 'biometric' data;
> (iii) the interlinking of alerts;
> (iv) widened access to the SIS II;
> (v) a shared technical platform with the Visa Information System.

They are discussed in more detail in this study. The later is commented in subsection 4.4 on widened access.

4.1 The addition of new categories of alerts.

As a starting point we will need to look at the definition of "alert" given in Art. 3 (1), a) of the two legal instruments:

> 'alert' means a set of data entered in SIS II allowing the competent authorities to identify a person with a view to taking specific action.

In the field of police cooperation the definition also includes a set of data on objects, with the same purpose: to allow the competent authority to identify a person or an object in order to take specific action.

[74] Hayes, B., *Supranote 25*, p.3.

All types of the existing alerts under CIS will be entered into SIS II, but the texts are revised.

The two legal instruments establish different types of alerts in accordance with the fields of the EU legal framework they regulate.

The SIS II Regulation in Article 24 establishes rules on the alerts for refusing entry and stay of third country nationals. Both alerts are issued on the grounds of a national alert resulting from a decision taken by the competent administrative authorities or courts. Such decision is taken in accordance with rules of procedure laid down by national law and on the basis of an individual assessment. In Article 21 there is a proportionality requirement "the Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II" Both the individual assessment and the proportionality requirements are guarantees for entering an alert but are regulated by national rules of the Member States, thus differences will exist. This is not beneficial for personal data protection. Some alerts entered in the system by one Member State would not be considered to meet those criteria by other/s Member State/s or vice versa. Concomitantly, the restriction of entering and/or stay applies to the whole Shengen area, i.e. the territories of all Member States.

The alert related to restriction of stay was proposed by the European Parliament (EP) with the wording "[…] or residence within […]"[75] and was finally adopted with the wording "[…] or stay […]" in Article 24 of the SIS II Regulation.

[75] The Draft Report on the proposal by the Commission for Regulation of the European Parliament and the Council on the establishment, operation and use of the SIS II, 31.3.2006, (COM(2005)0236 – C6-0174/2005 – 2005/0106(COD)), para 1.

"Stay" has a broader meaning since it does not relate only to persons who have acquired a residence permit or intend to do so, but to all who stay on the territory of a Member State. In this way it broadens the discretionary power of the Member States in relation to all third country nationals who happen to be on their territories.

In Article 24(1) and (2) of the SIS II Regulation the national alert is based on a decision taken by the competent administrative authorities or courts and the latter is taken in cases when "based on a threat to public policy or public security or to national security […]" posed by the presence of the third country national in question and in particular in the case of:

> […]
> b) a third-country national in respect of whom
> there are serious grounds for believing that he has
> committed a serious criminal offence or […]
> there are clear indications of an intention to
> commit such offence in the territory of a Member State.

These grounds for a decision of the competent national authorities are "broad and vague" and "they raise issues of proportionality as persons could be registered on questionable political grounds."[76] Sometimes there might be registration by mistake and innocent people may experience negative consequences on their right to privacy.[77]

Statewatch criticized this text because it remains almost identical to the present text of Article 96 CIS and no requirement exists for showing a "serious" threat to public

---

[76] Karanja, S., *Supranote 52*, p. 89.

[77] The Article 96 Inspection, Report of the Schengen JSA on an inspection of the use of Article 96 alerts in SIS; the conclusion identifies three categories of problems in relation to the content of the Article 96 alerts: 1. Alerts not in conformity with the national law; 2.Errors when entering the final date of the alert […]; 3. Alerts on nationals of EU Member States, p.8.

policy. The threshold for issuing an alert on the latter grounds is lowered. Presently CIS refers to 'clear evidence' of an intention to commit serious crimes, while the SIS II Regulation requires only 'clear indications' of such an intention (Article 24 (2), b)).[78] The final text reads that there must be "serious grounds for believing" or "clear indications of an intention" which cannot be qualified as evidence that serious criminal offence has been committed or intended to be committed by the data subject. The text of the same article provides no definition of "a threat to public policy or public security or to national security" and their meaning and content will be clarified under the national law of each Member State. This presupposes that national lists of threats with broader or narrower classification will exist and consequently result in different grounds for registration in SIS II. This will not benefit the protection of the right to personal data protection of data subjects at the EU level. It creates a basis for a variety of grounds for entering alerts on third country nationals with the purpose of refusal of entry or a stay within the territory of a Member State and effectively for the whole Schengen area.

An illustration of this situation is the practice in Germany: people whose asylum application has been rejected are registered under Article 96 CIS. Another example is the practice in Italy to register persons en masse simply because they are not welcomed immigrants on the same grounds.[79]

A further example from German practice is a case with a person from Bosnia and Herzegovina who applied for asylum for the first time in 1994 in Germany. Subsequently he was found to have a fake French Schengen visa and prosecuted for falsifying legal documents. In 2003 after the criminal charges were dropped he was expelled from Germany and recorded in the N.SIS with the purposes to refuse

---

[78] Statewatch briefing paper on Schengen Information System II: Immigration Regulation, October 2006, p.7, available at: http://www.statewatch.org/news/2006/oct/11eu-sis-II-sources.htm, accessed on 19.11.2010. The final text was adopted with those terms as in the draft.

[79] Karanja, S., *Supranote 32*, p.213.

entry. The record was not deleted on the grounds that the suspected criminal behavior of the person concerned would imply a threat to security and public order. The court ruled that the registration was not in accordance with Article 96 CIS and ordered the data to be deleted, since the registration was based on suspicion which did not meet the threshold of a crime.[80]

The Joint Supervisory Authority (JSA Schengen) stated that "Policy makers should consider harmonizing the reasons for creating an alert in the different Schengen States"[81] with respect to Article 96 CIS. This obviously was not taken into account in Article 24 of the SIS II Regulation. The possibilities for broad interpretation of the grounds for entering alerts under this article remain.
The importance of these alerts was underlined by the EDPS. He stated that the alerts issued in respect of third country nationals for the purpose of refusing entry have a significant impact on the freedoms of the individual since she/he has no more access to the Schengen area for several years.[82]

Third country nationals can file appeals against the decisions of competent national authorities and these appeals "shall lie in accordance with national legislation", Article 24 (1). This opportunity is positive development for personal data protection.[83] It still raises some questions, for instance how an appeal against such a decision shall be filed and revised if the third country national applies for visa to

---

[80] Verwaltungsgeright Berlin, 3 December 2004, Az.1 A 151.04., Brouwer, Evelien (2008), *Digital Borders and Real Right*, Martinus Nijhoff Publishers, 2008. p.p. 432,433.

[81] Article 96 Inspection, Report, *Supranote 77*, p.9.

[82] EDPS, *Supranote* 9, para 4.4.1., p .47. It comments the 2005 draft of the Regulation, but is relevant to the final text in this part.

[83] Karanja, S., *Supranote 52*,p.p. 89-90.
The article comments on the first drafts of the SIS II legal instruments of 2005, but is relevant in many points to the final texts.

enter the Schengen area, when he/she is outside it;[84] how long should it take and how much should it cost? It seems to be clumsy, costly and burdensome for a third-country national. All this might have dissuasive effect upon the third country nationals to appeal the decisions of foreign administrative authorities or courts and may have negative implications on the right to data protection. On the other hand it opens the possibility for forum shopping.

Separate conditions for issuing alerts under Article 15 of the TEU exist, including measures implementing a travel ban issued by the Security Council of the United Nations (Article 26 of the SIS II Regulation). There are unspecified and unclear criteria on the data to be entered, Article 26 (2) states that the "Article 23 'Requirement for an alert to be entered' shall not apply." The latter provides a list of data without which an alert may not be entered. There is no list of data that must be entered to constitute alert under Article 26. One guess could be that it allows either more or less data to be entered than listed in Articles 20 and 23. There are no clear indications in the text for any of these speculations but still one result may be that the principles of proportionality and minimality of data protection laws could be infringed.

Alerts under the SIS II Decision, third pillar, are greater in number and type than in the first pillar. More concerns from the point of view of data protection standards arise in the course of work of the competent authorities for judicial and police cooperation. The Member States have regulated the personal data collection, use and protection in this field at the national level, taking into account the CoE Convention and the non-binding Recommendation No.R (87) 15. They need to align their national laws with the most recently adopted Framework Decision

[84] EDPS, *Supranote 9*, para 6.4., p. 50.

2008/977/JHA, but the latter is not aligned with the CoE Convention and made no big difference to the *status quo* (see Subchapter 3.2.)

The alerts to be entered under the SIS II Decision are:

- Alerts in respect to persons wanted for arrest for surrender or extradition purposes, Chapter V;
- Alerts on missing persons, Chapter VI;
- Alerts on persons sought to assist with a judicial procedure, Chapter VII;
- Alerts on persons and objects for discreet or specific checks, Chapter VIII;
- Alerts on objects for seizure or use as evidence in criminal proceedings, Chapter IX.

The SIS II Decision introduces rules on objectives and conditions for the issuance of each category of the above stated alerts giving specific rules for entering of each alert in line with the purposes it serves. This makes the entering of different alerts more comprehensive and at first sight in line with the principle of fair and lawful processing of data.[85] However, there are rules on entering additional and supplementary information, which in some cases might allow too much as well as sensitive personal data to be collected and processed. From the point of view of the data protection principles of fair and lawful processing, proportionality and minimality of particular concern are texts as in Article 29 (1), f) of the SIS II Decision: "any other information useful or necessary for the execution of the alert." They open the possibility for exchange of a broad amount of personal data.

[85] Bygrave, L., *Supranote 3*, this is a "primary principle" in data protection because it embraces and generates the other core principles of data protection laws, p. 58.

There are cases where access to personal data is expanded to Europol and Eurojust. This fact poses difficulties in observing the purpose limitation principle since these organisations may access data for the performance of their tasks (Article 43 of the SIS II Decision), which are not always the same with the purposes of SIS II for processing of personal data.

The supplementary information shall be exchanged in accordance with SIRENE Manual which has not yet been adopted. Additional and often lengthy procedures might lead to time gaps where important issues of data protection stay unregulated. Time gaps without adequate and detailed rules presuppose that the right to data protection is not fully guaranteed in SIS II.

The information of EAW shall be communicated in regard to alerts on persons wanted for arrest for surrender purposes and those wanted for arrest for extradition purposes (Articles 28 and 29 of the SIS II Decision). In both cases the EAW shall be exchanged as supplementary information. The personal data scope in these cases is expanded by the inclusion of the EAW.

Article 27 of the Decision requires a copy of the EAW to be exchanged as "additional data" to the alerts for surrender purposes which are on the basis of EAW. Additional data are stored in the CS-SIS II and are accessible by all Member States' competent authorities and also by Europol and Eurojust in the third pillar data processing.

The processing of the sensitive categories of data listed in the first sentence of Article 6 of the CoE Convention is prohibited according to Article 56 of the SIS II Decision. There could be an exchange of information leading to processing of sensitive categories of data, when for example reading information such as place

and date of birth, nationality and a reference is made to the decision giving rise to the alert (Article 20 (3) c) g) and k) of the SIS II Decision). Such information could reveal racial origin, political opinions or other beliefs which are sensitive categories of data related to a person. The SIS II Regulation has the same texts in Article 20 and Article 40 prohibits the processing of the sensitive categories of data listed in Article 8 (1) of Directive 95/46/EC. Thus, the same conclusion, that sensitive categories of personal data could be processed in SIS II, is valid.

4.2 New categories of data will be entered in SIS II.

The main change in comparison to the present SIS concerning personal data to be entered is the inclusion of biometric data - photographs and fingerprints, as well as the information of the EAW and the information from links between alerts.

The involvement of biometric data into SIS II has raised many concerns and in particular those related to their stability, accuracy, their impact on the right to privacy, the reliability of the techniques used for their collection and processing and fears of function creep. The general concern is that biometrics will be used for purposes other than those envisaged and – agreed - at the time of introduction.[86] The EDPS, Mr. Peter Hustinx, underlined that biometrics are inherently sensitive in nature and need adequate safeguards. He proposed that it would be useful to build a set of common obligations or requirements.[87]

The Commission Joint Research Committee (JRC), which functions as a reference center of science and technology for the EU, made in 2005 a research on the future

[86]Technical Report Series (2005), Biometrics at the Frontiers: Assessing the Impact on the Society for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (LIBE Committee), p.p. 115-119.

[87] EDPS, *Supranote 9*, para 4.1., p. 44.

impact of biometric technologies. It stated that the overall impact of the study is that "[…] it poses challenges to the way our society is organized, and these challenges need to be addressed in the near future if policy is to shape the use of biometrics rather than be overrun by it."[88]

The enrolment and use of biometrics currently for photographs and fingerprints, and for a later stage DNA and retinal scans[89] following necessary amendments change qualitatively SIS II and require adequate safeguards for such data.

The rules for photographs and fingerprints in Articles 22 of the SIS II Regulation and Decision state that they shall only be entered: i)following a special quality check to ascertain the fulfillment of a minimum data quality standard (it shall be established in accordance with a separate procedure regulated in Article 51(2) of the SIS II Regulation and in Article 67of the SIS II Decision; ii) the photographs and fingerprints shall only be used to confirm the identity of a person (one-to-one check) and iii) as soon as it becomes technically possible fingerprints may also be used to identify a person on the basis of his biometric identifier (one-to-many).[90]

The use of biometrics for one-to-many checks, which will not be used in the SIS II until the necessary technique is available, is more controversial. It imposes greater risks for misidentification than its use for one-to-one checks. It is less reliable than the latter since there might be positive or negative identification/false identification or false non-identification of a person.

The EDPS noted that: "Biometric data are 'live' data which evolve with time; the samples which are stored in the database constitute only a snapshot of a dynamic

---

[88]Technical Report Series, *Supranote 86,* p.119.

[89] House of Lords, *Supranote 47,* para 57.

[90] One -to -one check or verification ensures that the person X is really who he /she claims to be; one-to many check or identification discovers the identity of an individual, a central database is necessary with records for all people known to the system. Technical Report series, *Supranote 86,* p.p.38,39.

element."[91] Thus the biometric data cannot provide 100% security for identification purposes.

Function creep is one of the main fears related to the use of biometrics and combined with the possibilities for deviation from the purpose limitation principle in SIS II it raises the issue of adequate and efficient guarantees. Moreover, biometrics may provide secondary health data. [92]

There is a possibility of a fallback of a system and appropriate procedures in such instances should be adopted in order to protect individuals from imperfections of the system.

From the point of view of *de lege ferenda*, biometrics must not be used as the only method for identification. It would be more correct to have other data (names, date of birth, etc.) and/or a source for cross checks with initial information about a person. They could be done randomly or on a case by case basis, or when there could be serious consequences for the right to privacy of an individual.
The overall conclusion is that the use of biometrics for identification purposes should not be overestimated and adequate safeguards should be adopted before their use in practice in SIS II.

As mentioned above, the EAW which contains sensitive categories of data shall be entered in SIS II.[93] Supplementary data will not be stored in the CS- SIS II, but in the N.SIS II of the concerned Member States. This will have a restrictive effect as the data from the EAW will be available only to them. However, in some cases it is

---

[91] EDPS, *Supranote 9*, para 4.1, p.44.

[92] Technical Report, *Supranote 86*, paras 2.2.; 2.2.1; and 2.2.2, p.p. 50-51 .

[93] Framework Decision 2002/584/JHA, *Supranote 59.*

communicated to all Member States. The prohibition for processing of sensitive categories of data is not observed.

Additional data are registered in SIS II for the purpose of dealing with misused identity (Article 36 of the SIS II Regulation and Article 51 of the SIS II Decision). The registration of these data is positive for personal data protection since the explicit consent of the data subject, whose identity is misused, is required and the purpose is well defined: to help to distinguish the victims of misappropriated identity from those who are targeted by the alerts.

The new personal data to be added in SIS II raises some questions on their minimality / proportionality and purpose limitation and it is doubtful that the system has to cumulate such broad information, including sensitive data. The purpose of SIS II is to ensure a high level of security within the AFSJ by exchange of information communicated via the system. The exchange of information appears to be the main guarantee for ensuring a high level of security. Finding an optimal balance between security and personal data protection is crucial. The best would be if it is estimated on a case by case basis taking into account the relevant conditions. This approach will require more efforts, resources and time than a holistic one.

4.3 The interlinking of alerts.

There are rules on how links between alerts may be created (Article 37 of the SIS II Regulation and Article 52 of the SIS II Decision). The effect of such a link shall be to establish a relationship between two or more alerts, a function not available in the current SIS. The introduction of this new function will make it possible for different data to be interlinked for one or more persons and/or objects. It certainly will be very useful for control purposes. However, for data subjects and their rights

to privacy and data protection it imposes a significant threat. Individuals will no longer be assessed only on the basis of data related to them but also on the basis of data on other persons, and/or objects, who might be criminals or suspected in criminal activities.[94] That function creates a pool of interlinked information in the CS-SIS about different subjects and objects interlinked, sometimes under accidental circumstances of the daily life and having nothing to do, with illegal activities. Thus, innocent people can be related to criminals and illegal activities and become suspects. There is a requirement in accordance with which Member States create a link between alerts only when there is "a clear operational need"[95] as well as a requirement that the creation of a link shall not affect access rights of the competent authorities.[96] The first requirement will be clarified under the national law of Member States, so there will be a variety of interpretations of what is a clear operational need. The second requirement is adequate from the point of view of the purpose limitation principle, since the access rights of all authorities which work with the system are established to the extent they are able to fulfill their tasks.

The EDPS [97] recommended that those authorities that do not have a right of access "should not even be aware of the existence of these links." This result seems to be achieved since they cannot access the information related to links not in the ambit of their competence. The technical rules for interlinking alerts shall be adopted in accordance with the "comitology procedure" (Article 37 (7) of the SIS II Regulation and Article 52(7) of the SIS II Decision).

---

[94] EDPS, *Supranote 9*, p.46, para 4.3.

[95] Cf. Article 52 (4) of the SIS II Decision; Article 37 (4) of the SIS II Regulation.

[96] *Ibid.* Articles 52 (3) and 37 (3).

[97] EDPS, *Supranote 9*, p.47, para 4.3.

Searches will be possible at the national and at the central level of SIS II. In the current system this is done only at the national level; the central system is simply an index system and does not store data.[98]

A national copy shall be available for the purpose of carrying out automated searches in the territory of each of the Member States, Articles 4 (2) of the SIS II Regulation and Decision. The making available of a national copy is encompassed by the term "processing" defined in Article 3 (1), e) of the SIS II Decision and in Article 3, f) of the SIS II Regulation.

The availability of information is a principle introduced by the Hague Programme.[99] The impact of the 9/11 attacks was well reflected in it, strengthening security was an important element and so was the improving of the exchange of information. The availability principle became a priority. It means that if data is held in one national system then it can be shared between the law enforcement agencies of all Member States for the purposes of combating terrorism and fighting organized cross-border crime. Thus, personal data is available on the territory of each Member State and will be used by law enforcement agencies in their fight against terrorism and organized cross-border crime. It will be difficult to trace which is the authority or how many of them are processing the personal data at a particular moment.

4.4 Widened access to SIS II.

In the beginning the access to the current SIS was allowed for border control authorities, police, customs officials and immigration authorities within the scope

[98] Karanja, S., *Supranote 52*, p.85.

[99] The Hague Programme *Supranote 17*, p.27.

of their competences. Later on Council Regulation 871/2004/EC and Council Decision 2005/211/JHA concerning the introduction of some new functions for the SIS, in particular the fight against terrorism were adopted. They widened access rights to Europol and the national members of Eurojust to data stored in the current SIS.

The new legal instruments on SIS II regulate access rights to Member States' national judicial authorities, Eurojust - the EU Prosecutions Agency, a judicial cooperation body created to help provide safety,[100] Europol - the European Police Office[101] and the vehicle registration authorities.[102]

The widened access to personal data in SIS II can be discussed, inter alia, through the implementation of the availability principle since it opens access for the purposes of fighting crime and terrorism for all competent national authorities. They will differ in number for different Member States since are designated by each Member State under its national law.

The EDPS has taken the view that "access must be granted to authorities in full compliance with the general purpose of SIS II and with the specific purpose of each alert" on the condition they have specific competence to take action on a specific alert. [103]

Europol has long sought access to SIS with the argument that it needs these data for its analyses on "organized crime". The purpose of making analyses is not among

---

[100] *Supranote 67*.

[101] *Supranote 68*.

[102] Article 27 of the SIS II Regulation, Articles 40,41 and 42 of the SIS II Decision and the Regulation 1986/2006/EC.

[103] EDPS, *Supranote 9*, para 4.2.1, p. 44.

those included in the SIS purposes,[104] although it might prove useful for security and control purposes and particularly for prevention of illegal activities.

The European Council adopted a *Declaration on combating terrorism* on 25 March 2004, right after the terrorist attacks in Madrid, and called the Commission to submit proposals for enhanced interoperability between SIS II, VIS and Eurodac for preventing and combating terrorism.

Article 41 of the SIS II Decision reads that Europol shall within its mandate have the right to access and search data entered in accordance with the stated alerts.
Europol may use the information obtained from a search in SIS II after the consent of the Member State which issued the alert. Europol handles the information and may request further information from the Member State in accordance with the Europol Convention, Article 41 (3; 4) of the SIS II Decision.

The positive element for personal data protection is that it shall record every access and search made in the system, shall not connect parts of SIS II nor transfer the data contained therein nor download or otherwise copy part of SIS II, the access shall be limited to specifically authorized staff.
The negative is that the Joint Supervisory Body set up under Article 24 of the Europol Convention shall review the activities of Europol. It is a supervisory authority different from EDPS.

Access to SIS II by Eurojust is regulated by Article 42 of the SIS II Decision in a similar way as for Europol. For both access rights are limited by their mandate. Article 43 of the SIS II Decision defines the scope of their access rights "[…] only […] for the performance of their tasks." Their access rights are further limited by

[104] Hayes, B., *Supranote 25*, p.6.

the types of alerts they will have access and search rights to, and the consent of the Member State that has entered the alert for Europol, and the obligation to inform the Member State that has entered the alert for Eurojust.
The EDPS stated that access can in any case be granted only when it is compatible with the general purpose of SIS II and is in accordance with its legal basis.[105]

There is a lack of clear purpose specification for the right to access and search directly into personal data entered to SIS II. The requirement is that Europol and Eurojust can access data in SIS II within their mandate. There is no requirement that their access rights to SIS II data is conditional upon executing an action based on a specific alert for example. Thus, they can access and use the SIS II data for purposes other than those defined in the SIS II Decision and/or different from which the data were collected initially. In any case there is a need for compatibility with the purposes of SIS II but this is not guaranteed by the SIS II legal texts.

For both Europol and Eurojust there is a possibility to communicate the information obtained through a search of the system to third countries and third bodies with the consent of the Member State which issued the alert, Article 41 (3) and Article 42 (2) of the SIS II Decision despite the general prohibition for transfer of personal data from SIS II to third countries or to international organisations in Article 54.

The requirement that they will have the right to access data in SIS II with the purpose of performing their tasks serves as a restriction itself to their access rights. This is in line with the scope of their work but not with the core principle of purpose specification or limitation of data protection laws and more so with the SIS II rules. The use of personal data obtained from SIS II can deviate from the

[105] EDPS, *Supranote 9*, para 4.2.2., p 45.

purposes for which they were initially collected and can lead to starting the processing of personal data anew. The communication of information to third countries and bodies will make it difficult to establish which country and body is processing specific personal data at a given moment.

The supervision of the use of SIS II personal data by Europol and Eurojust is governed by other legal instruments and other supervisory authorities – the Joint Supervisory Body set up under Article 24 of the Europol Convention for Europol and the Joint Supervisory Body set up pursuant Decision 2002/187/JHA for Eurojust. Thus, the control and supervision activities are complicated.

From *de lege ferenda* point of view the SIS II Decision could have provisions on meetings between all supervisory authorities at a central level, EDPS, Joint Supervisory Body Europol and Joint Supervisory Body Eurojust with a purpose to discuss issues connected to processing of personal data in SIS II.

The authorities responsible for issuing certificates of vehicle registration are granted access to the SIS II information by the adoption of Regulation 1986/2006/EC in order to properly issue the certificates, thus the purpose is clearly stated. The access of the competent authorities for registration of vehicles seems to be the most uncontroversial one since it is necessary for the performance of their tasks (Recitals 7 and 8 of the Regulation 1986/2006/EC).

The Visa Information System (VIS) was established in the first pillar by the adoption of Decision 2004/512/EC 8 June 2004 establishing the Visa Information System.[106]

[106] OJ L 213/5, 15.6.2004.

The VIS was the first police and border control electronic system established in the aftermath of 9/11 and clearly reflects the will of the European politicians and lawmakers to take more adequate and advanced measures that guarantee security. This system was established in the context of the common visa policy of the Member States. It was approved that biometric data will be entered into VIS. Another database is EURODAC[107] established with the purpose to assist in determining which Member State is to be responsible pursuant to the Dublin Convention[108] for examining an application for asylum lodged in a Member State and otherwise to facilitate the application of the Dublin Convention. Both data bases have nothing to do with police and law enforcement issues.

The Commission noticed the lack of law enforcement access to VIS as a shortcoming and a serious gap in the identification of suspected perpetrators in the prevention and fight against serious crime and terrorism. This shortcoming was identified by the Commission in relation to EURODAC, also a first pillar tool.[109]

As a result of this, Council Decision 2008/633/JHA of 23 June 2008 was adopted, dealing with the access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.[110]

---

[107] Regulation 2725/2000/EC, 11 December 2000, concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Dublin Convention, OJ L 316/1, 15.12.2000.

[108] CONVENTION determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities (97/C 254/01); OJ C 254 , 19/08/1997 p. 1 – 12.

[109] Communication from the Commission […] on improved effectiveness, enhanced interoperability and synergies among European databases in the area of JHA, 24.11.2005, COM (2005) 597 final, para 4.6, p.6.

[110] OJ L 218/129, 13.8.2008.

There is a clear incompatibility with the purpose limitation principle for the designated authorities which may access the data in the VIS, where the first reason for collection of personal data is connected first and foremost to the processing of visa applications. The EDPS stated that strict requirements and limits for this additional access should be followed such as granting access to law enforcement authorities only in specific circumstances, on a case by case basis and accompanied by strict safeguards.[111] De Busser[112] pointed out that the access for the purposes of combating crime and terrorism does not constitute use for a compatible purpose and concluded that it can be considered compliant with the requirements of lawful derogations to the purpose limitation rule according to the CoE Convention, Art. 9 (2) " […] such derogation is provided for by the law of the Party and constitutes a necessary measure […] in the interests of: a) protecting State security, public safety […]".
It can be an exception according to Article 13 (1) of Directive 95/46/EC in the field of first pillar processing of personal data.

EURODAC is a fingerprint data-base and its data could be accessible for authorities other than those which examine an application for asylum lodged in a Member State after its adjustment for this purpose.

In his opinion on the proposals for a Council Decision[113] and a Regulation[114] the EDPS[115] stated that measures to combat terrorist offences and other serious

[111] EDPS opinion 20 January 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences (COM (2005) 600 final), p.3.

[112] De Busser, E., *Supranote 71*, p.180.

[113] Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM (2009) 344 final, 10.9.2009.

offences can be a legitimate ground for allowing processing of personal data, provided that the necessity of the intrusion is supported by clear and undeniable elements. He also underscored the need for higher protection of asylum seekers because they flee from persecution and the risk of stigmatization.

EURODAC and VIS were not intended to be data bases for law enforcement purposes and the visa and asylum seekers are not by definition linked to terrorism or serious crimes so that their data need to be made available to the law enforcement authorities of the Member States and Europol. Moreover, both contain highly sensitive data – biometrics.

4.5 Summing up.

The new functions of SIS II enormously expand its effectiveness in personal data collection and use, changing the characteristics of the system from a hit/no hit to an investigative tool. The concerns over the right to data protection and its guarantees are not without grounds. The latest political developments created a good

---

[114] Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), COM (2008) 825 final, 3.12.2008.

[115] Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…)(establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, para 53.; OJ C 91/1, 10.04.2010, p.8.

justification for the introduction of new security measures making it possible new personal data to be collected and processed using the most developed technologies. The expanded access to information entered into SIS II under both pillars poses a threat to the purpose limitation principle and to the fair and lawful gathering and processing of personal data. Some important rules are left to be adopted at the national level, leading to a lack of consistency, for instance the grounds for entering alerts on refusal of entry or stay of third country nationals. This lead to registration of alerts in SIS which do not fulfill the legal criteria for entering alerts as in the case with the person from Bosnia and Herzegovina registered in the German N.SIS (subchapter 4.1).

The new categories of data such as biometrics and the EAW contain sensitive data that can be collected and processed in violation of the prohibition for processing of such data. There are no clear rules for the special quality check needed for entering biometric in SIS II and for the interlinking of alerts. They will be subject to comitology procedure, so there will be time gaps without necessary specific regulation. The fight against terrorism and organized crime triggered new rules on SIS II to be provided. They not only maintain the *status quo* established by the current SIS with prevailing security concerns over the right to privacy but additionally elaborate the security measures while the data protection rules lag behind. Moreover, the purpose of SIS II to ensure a high level of security within the AFSJ of the EU challenges the European lawmakers to ensure security while lowering the value of right to privacy. The terrorist threats and organized crime find their counter strike in the EU and Schengen in new and more elaborate legal rules allowing the competent authorities to collect and process more and more data using the most advanced technology while the safeguards for the fundamental right to data protection are not developed with the same speed and sophistication. This tendency has been primarily clear in the third pillar data processing. It also finds place in the first pillar data processing via the SIS II where the level of personal

data protection is not consistent with that provided by Directive 95/46/EC and there are opportunities for access to the SIS II data collected for visa and asylum purposes. The third pillar data protection standards do not follow up those in the CoE Convention. Tthey are lower and looser.

Both sides of the coin - security and data protection are reflected in the new SIS II legal rules. The prevalence of security, however, gets more attention quantitatively and qualitatively over data protection.

5 Conclusion.

There are new documents approved in the EU. They give glue about the future interrelationship between security and data protection. As for example the Stockholm programme. It makes reference to the definition of a comprehensive, internal security strategy.[116] Among its principles are stringent cooperation among EU agencies, including further improving information exchange and the use of regional initiatives and regional cooperation.

The Prüm Treaty, referred as Schengen Information System III (SIS III), signed on 27 May, 2005 by some Member States provides for facilitation of police cooperation including the mutual exchange of DNA profiles, fingerprints, etc. It was adopted in the EU legal framework by Council Decision 2008/615/JHA of 23 June 2008 (Decision 2008/615/JHA)[117] on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. It extended information exchange outside the EU framework based on principle of availability. Data which is exchanged includes sensitive data. This legally binding instrument clearly demonstrates the contemporary relationship between security and data protection where security goes first. In the third pillar the Member States have demonstrated little willingness to harmonise the data protection rules. This was further demonstrated by the adoption of Framework Decision 2008/977/JHA.

The question that arises is whether the rules and procedures in SIS II are appropriate and consistent with the ambition for high level of data protection in the EU. The broad amount of personal data which is allowed to be entered and exchanged between Member States and in some instances with third countries and third bodies is not positive for data protection in the third pillar. There is lack of

[116] Stockholm Programme, *Supranote 17,* p.p. 35,36.

[117] OJ L 210/3, 6.8.2008.

harmonized, comprehensive and common legally binding criteria. In the first pillar the new rules of the system do not fully follow the pattern of the Directive 95/46/EC rules. In the third pillar the new rules do not add any value to the *status quo.* On the contrary they show the eagerness of the Member States to keep and develop it.

This gives rise to other thoughts as for example, do we have the right and up-to-date data protection standards for the purposes for which personal data need to be gathered and processed in SIS II? Especially in the police and judicial co-operation areas. Do we need to rethink some of our fundamental human rights such as the right to privacy and data protection in accordance with the new challenges posed by the contemporary political and technological developments? Do we need to rethink the principles of data gathering and processing making them in line with the new needs for security measures?

In 1985, in the White Paper on the Internal Market, the Commission underlined the symbolic meaning of borders. The notion of a free movement area has been steadily developed in an environment of novelties. The political aims and plans have been changed accordingly. In the beginning of the current SIS, as Brower pointed out, the Commission did not foresee the development of high- tech control and surveillance measures to which individuals traveling around Europe are now exposed. And a question arises as to whether these new measures are not precisely the same as those the Commission tried to abandon in 1985.[118] I would add that the Commission could not foresee the whole range of political developments in particular terrorist activities and their impact over the notion of security. The new measures in the name of a high level of security within the AFSJ of the EU in reality pose more threats to the fundamental right to data protection than those imposed some 25 years ago. Gathering of personal data becomes easier and

[118] Brouwer, E., *Supranote 80,* p. 534.

undetectable and the willingness of the Member States to take advantage of this is growing when security is concerned.

The SIS in the EU has been created with the main purpose to compensate for the lack of regular border checks and control. Security concerns and the right to data protection can come across as the two sides of one coin whose interrelationship is such that while one of them increases in value the value of the other diminishes. Concomitantly, the possibility to achieve a balance between the two, considering the background of the political developments from the last decade, requires efforts and political will in order adequate safeguards to be appointed. This balance cannot be based on equality, but rather on optimization of the two sides on the basis of revised and updated rules. The security concerns have prevailed steadily in the regulation of the SIS and SIS II functioning. This tendency must be curbed so that we do not end up with a stronger and stricter and often not legally justified border control and surveillance than we had before 1985. This would significantly affect the trust model between the citizen and the state, respectively the citizens and the EU, a model that has been established in the European Western democracies and admired by many East European countries.

The Stockholm programme states that developments over the past years in the EU have led to a wide choice and created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of freedom, security and justice.[119] Concomitantly it invites the Council and the Commission to implement an EU Information management strategy with a strong data protection regime.

Undoubtedly there is a need to keep and sometimes to increase the value of the security side of the coin, but we must not forget to preserve and observe the

[119] Stockholm programme, *Supranote 17*, p.37.

protection of the fundamental human rights like the right to data protection by accepting adequate and efficient safeguards. Such safeguards are not present in the SIS II legal tools. There are no rules for example, on the quality check for biometric data, the data subject rights are not comprehensively regulated, and the systems' new functions have the potential to undermine the basic principles of data protection. There is a risk to minimize the data protection side to negligible levels in SIS II. The political landscape constantly changes requiring optimal security measures which would instill confidence in the data subjects without minimizing the value of their fundamental human rights. The optimization of interrelationship between security and personal data protection would guarantee a stable model for all democratic European countries.

A positive development for personal data protection is the Communication from the Commission on a comprehensive approach on personal data protection in the EU of 4.11.2010.[120] It states that its aim is to revise the personal data protection standards in Europe while keeping up with the latest political and technological developments.

[120] Brussels, 4.11.2010, COM (2010) 609 final.

References

Treaties/Statutes

Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28.01.1981.

Convention Applying the Schengen Agreement of 14 June, 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany, the French Republic on the Gradual Abolition of Checks at Their Common Borders, 1990.

Treaty on European Union, 1992 (Maastricht treaty).

Treaty on European Community, 1992 (Maastricht treaty).

Europol Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office, 1995.

The Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, 1997.

Protocol Annexed to the Treaty of Amsterdam Amending the Treaty on European Union the Treaties Establishing the European Communities and Certain Related Acts, 2 October, 1997.

Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, 1997- Dublin Convention.

Charter of Fundamental Rights of the European Union of 7 December 2000.

Convention 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Dutchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (Prüm Convention), 10900/05, 7 July, 2005.
Treaty of Lisbon amending the Treaty of the EU and the Treaty establishing the European Community, 2007 (The Lisbon Treaty).

Regulations / Directives / Decisions/ Recommendations

Recommendation No.R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Regulation 2725/2000/EC, 11 December 2000, concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Dublin Convention.

Regulation 45//2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Schengen Acquis, 2000.

Council Regulation 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II).

Council Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II).

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.

Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States.

Council Regulation 871/2004 of 29 April 2004 concerning the introduction of some new functions for the SIS, including the fight against terrorism.

Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System.

Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism.

Commission Decision of 22 September 2006 on amending Sirene Manual, Decision 2006/758/EC.

Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

Regulation 1987/2006 of the European Parliament and of the Council of 20 December 2006 on establishment, operation and use of the new SIS II.
Council Decision 2007/533/JHA of 12 June 2007 on establishment, operation and use of the new SIS II.

Council Decision 1999/468/EC laying down the procedures for exercise of implementing powers conferred on the Commission.

Regulation 1986/2006 of the European Parliament and of the Council regarding access to the Second Generation Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates.

Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of

Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).

Opinions/Reports/MEMOs

Commission Staff Working Paper on the Development of the SIS II, 2002 Progress Report, Brussels 18.2.2003, SEC (2003) 206.

Draft Report on the proposal by the Commission for Regulation of the European Parliament and the Council on the establishment, operation and use of the SIS II, Committee on Civil Liberties, Justice and Home Affairs, European Parliament, 31.3.2006, (COM(2005)0236 – C6-0174/2005 – 2005/0106(COD)).

Article 96 Inspection, Report of the Schengen Joint Supervisory Authority on an inspection of the use Article 96 alerts in the Schengen Information System, 20 June 2005.

Joint Supervisory Authority Schengen opinion of 27 September 2005 on the SIS II proposals.

Opinion of the European Data Protection Supervisor of 20 January, 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences (COM (2005) 600 final).

Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final); the proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final) OJ C 91/38, 19.4.2006.

European Data Protection Supervisor, Third opinion 27 April 2007 on the Proposal for a Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters, OJ C, 139/1, 23.6.2007.

Article 29 Data Protection Working Party, 01248/07/EN, WP 136, Opinion 4/2007 on the concept of personal data, 20 June 2007.

Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…)(establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes. OJ C 91/1, 10.04.2010.

House of Lords European Union Committee 9th Report on Session 2006-07.

Technical Report Series (2005), Biometrics at the Frontiers: Assessing the Impact on the Society for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (LIBE Committee).

Summary of the Working Party on SIS discussions, 6386/02, Brussels, 15.02.2002, available at: http://www.statewatch.org/news/2005/may/sources-SIS-to-SIS%20II-and-VIS.htm, last visited 4.09.2010.

MEMO /10/349, Brussels, 20 July 2010, EU Information Management Instruments, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/349&format=HTML&aged=0&language=EN&guiLanguage=en, last accessed on 17.11.2010.

Communications/Declarations

Communication from the Commission to the Council and the European Parliament, Development of the Schengen Information System II, COM (2001) 720, final, Brussels, 18.12.2001.

European Council Declaration on combating terrorism of 25 March 2004.

Communication from the Commission to the Council and the European Parliament, COM (2005) 597 final, Brussels, 24.11.2005, on improved effectiveness, enhanced interoperability, and synergies among European databases.

Communication from the Commission to the Council and the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609 final, Brussels, 4.11.2010 on a comprehensive approach on personal data protection in the European Union.

Conclusions/Action plans/Programs

Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice, Text adopted by the Justice and Home Affairs Council on 3 December 1998.

TheTampere Summit Conclusions, 15-16 October 1999 (The Tampere programme).

Presidency Conclusions European Council Meeting in Laeken, 14 and 15 December 2001.

Action Plan of 21 September 2001 against terrorism

The Presidency Conclusions, 4-5 November 2004 (The Hague programme).

The Stockholm Programme - An open and secure Europe serving and protecting the citizens, 2 December, 2009.

Secondary Literature

Bygrave, Lee A. (2002), *Data Protection Law: Approaching Its rationale, Logic and Limits,* Kluwer Law International (2002).

Brower, Evelien (2008), *Digital Borders and Real Rights, Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, 2008.

Bunyan, T. Statewatch analysis (2002), *The War on Freedom and Democracy: An analysis of the effects on civil liberties and democratic culture in the EU*, 6.9.2002.

De Busser, Els, (2009), *Data Protection in EU and US Criminal Cooperation, A Substantive law Approach to the EU Internal and Transatlantic Cooperation in Criminal matters between Judicial and Law Enforcement Authorities*, Maklu 2009.

Hayes, B. (2004), Statewatch Analysis, *From the Schengen Information System to SIS II and the Visa Information System (VIS): the proposals explained*, Statewatch Report February 2004.

Hayes, B., Peers, S. and Bunyan,T., Statewatch, (2004), *Scoreboard on post - Madrid counter-terrorism plans,*, 23 March 2004.

Hayes, B. (2005) Statewatch Analysis, *SIS II: fait accompli? Construction of EU's Big Brother Database Underway*.

Statewatch briefing paper on Schengen Information System II: Immigration Regulation, October 2006, available at: http://www.statewatch.org/news/2006/oct/11eu-sis-II-sources.htm,

Karanja, Stephen K. (2000), *The Schengen Cooperation: Consequences for the Rights of EU Citizens*, "Mennesker og rettigheter Årgang 18 Nr. 3, 2000."

Karanja, Stephen K. (2005), *SIS II Legislative Proposals 2005: Gains and Losses!*, YULEX 2005.

Karanja, Stephen K, (2006), *The Directive on Data Retention-Between Privacy and security*,YULEX 2006.

Karanja, S. K. (2008), *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, Martinus Nijhoff Publishers, 2008.

Michael, Katina and M.G, Michael, *Schengen Information System II: the balance between civil liberties, security and justice*, available at: http://works.bepress.com/kmichael/53/.

Mironenko, Olga (2009), *Air Passenger Data Protection, Data Transfer from the European Union to the United States*, submitted as a Master Thesis in the University of Oslo in autumn 2009.

Internet Sources

Privacy International
http://www.privacyinternational

Statewatch
http://www.statewatch.org

European Digital Rights
http://www.edri.org

Annex 1

Abbreviations:

AFSJ- Area of Freedom, Security and Justice

CoE – Council of Europe

CIS – Convention Implementing the Schengen Agreement of 14 June 1985

C. SIS - Central Schengen Information System

CS-SIS- Central Schengen Information System II

EAW-European Arrest Warrant

EC – European Community

EDPS - European Data Protection Supervisor

EP-European Parliament

EU-European Union

JHA-Justice and Home Affairs

JRC-Joint Research Committee

JSA-Joint Supervisory Authority

N.SIS-National Schengen Information System

N.SISII-National Schengen Information System II

NI-SIS- a uniform national interface

OECD-Organization for Economic Cooperation and Development

SIRENE-Supplementary Information Request at the National Entries

SIS – Schengen Information System currently operational

SIS II-Schengen Information System second generation

SIS III -Prüm Treaty

TEC-Treaty Establishing European Community

TEU-Treaty on European Union

VIS-Visa Information System

Annex 2

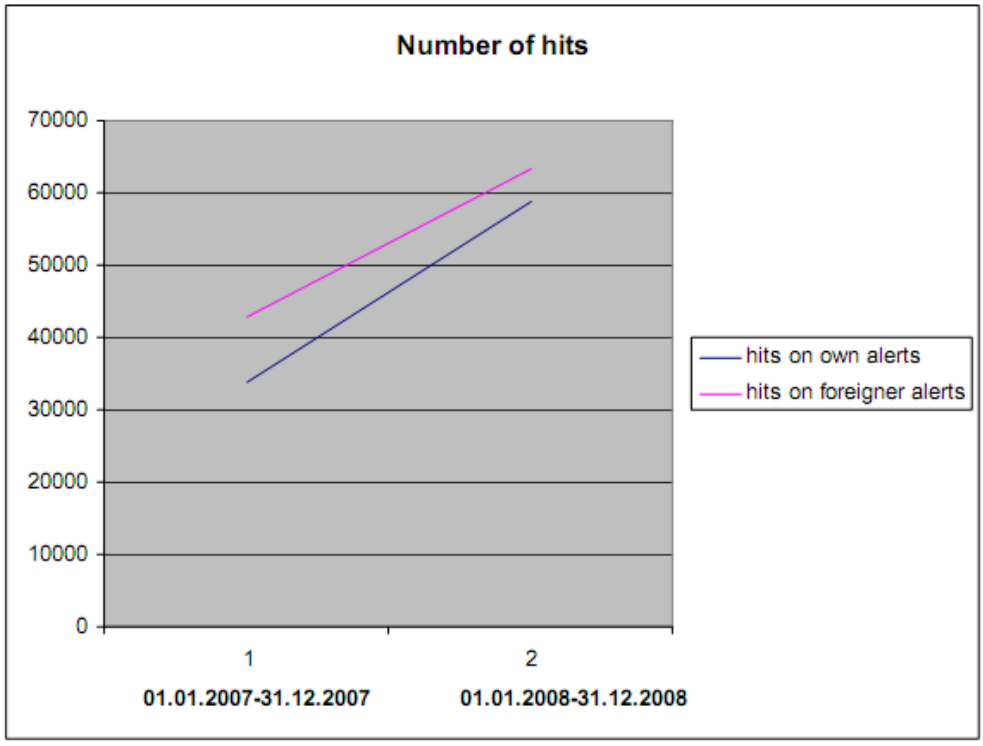
Alert categories	2007	2008	2009
Banknotes	177,327	168,982	134,255
Blank documents	390,306	360,349	341,675
Firearms	314,897	332,028	348,353
Issued documents	17,876,227	22,216,158	25,685,572
Vehicles	3,012,856	3,618,199	3,889,098
Wanted persons (aliases)	299,473	296,815	290,452
Wanted persons (main name)	859,300	927,318	929,546
Of which:			
Persons wanted for arrest for extradition	19,119	24,560	28,666
Third-country nationals on the entry ban list	696,419	746,994	736,868
Adult missing persons	24,594	23,931	26,707
Minor missing persons	22,907	24,628	25,612
Witnesses or persons subject to judicial summons	64,684	72,958	78,869
Persons subject to exceptional monitoring to prevent threats to public security	31,568	34,149	32,571
Persons subject to exceptional monitoring to prevent threats to	9	98	253

national security			
Total	22,933,370	27,919,849	31,618,951

MEMO 10/349, Brussels, 20 July 2010, EU Information Management Instruments, p. 3. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/349&format=HTML&aged=0&language=EN&guiLanguage=en, last accessed on 17.11.2010.

Annex 3

COMPARISON OF NUMBER OF OWN AND FOREIGN ALERTS IN PERIOD FROM 01.01.2007 TO 31.12.2007 AND FROM 01.01.2008 TO 31.12.2008



Council of the EU, 5171/09, LIMITE, SIRIS 7, COMIX 22, Brussels, 19 February, 2009, Annex 2.